Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. Please amend the claims as follows.

Listing of Claims:

1. (Currently Amended) In an initiating system, a computer-implemented method for establishing a new group identity, ~~with a group identity information document~~ the method comprising:

creating group identity information ~~for inclusion in the group identity information document~~;

selecting a first subset of the group identity information to include in a first group identity information document for disclosure to a first receiving system;

selecting a second subset of the group identity information to include in a second group identity information document for disclosure to a second receiving system, wherein the second subset is different from the first subset, and wherein the second receiving system is different from the first receiving system;

generating a first group-signed group identity information document comprising the first subset of the group identity information, an embedded use policy that expresses a privacy policy providing instructions as to how the first subset of the group identity information may be used, wherein the embedded use policy is stored with the first subset of the group identity information, at least a first key, and a first group identity information document signature signed by a group owner using a second key associated with the first key ~~in the identity information document~~, wherein the second key is a private key of the group and is owned by the group owner; [[and]]

sending the first group-signed group identity information document to [[a]] the first receiving system to establish the new group identity at the first receiving system.

2. (Cancelled)

3. (Currently Amended) The method of claim 1, further comprising:

sending a group-signed membership identity information document with the first group-signed group identity information document to the first receiving system to establish membership of an originator of the membership identity information document in the new group identity established at the first receiving system.

4. (Currently Amended) The method of claim 3 further comprising:

receiving the new group-signed membership identity information document from the originator;

detecting whether the group associated with the membership identity information document has been accepted; and

assigning security protocols to communications from the originator based on the first subset of the group identity information if the first subset of the group identity information is accepted.

5. (Currently Amended) The method of claim 3, wherein the act of sending comprises:

storing the group-signed membership identity information document in [[an]] the initiating system;

retrieving the group-signed membership identity information document;

attaching the group-signed membership identity information document to [[the]] a message; and

sending the message to the first receiving system.

6. (Currently Amended) The method of claim 3, further comprising:

sending to the first receiving system a self-signed personal identity information document of the originator ~~of the message~~ to establish at the first receiving system identity of the originator in addition to membership of the originator ~~originator's membership~~ in the new group.

7. (Currently Amended) The method of claim 6, wherein the acts of sending a self-signed personal identity information document and group-signed membership identity information document comprises:

generating the self-signed personal identity information document;

attaching the self-signed personal identity information document to [[the]] a message;

retrieving the group-signed membership identity information document;

attaching the group-signed membership identity information document to the message; and

sending the message to the first receiving system.

8. (Previously Presented) The method of claim 6 further comprising:

receiving the group-signed membership identity information document and the self-signed personal identity information document from the originator;

detecting whether the new group associated with the membership identity information document is accepted and whether the person associated with the personal identity information document is accepted;

assigning first security protocols to communications from the originator if the new group is accepted; and

assigning second security protocols to communications from the originator if the person is accepted.

9. (Currently Amended) In a communication system, an apparatus for establishing a new group identity comprising:

an initiating system, comprising a processing unit and computer storage media, the computer storage media encoding modules for execution by the processing unit, including:

a group ID generate module generating a group certificate comprising at least a public key, a digital signature for the group, and an embedded use policy that expresses a privacy policy providing instructions as to how a first subset of group identity information may be used at a first receiving system, wherein the embedded use policy is stored with the first subset of group identity information and wherein the first subset of group identity information is selected from group identity information for disclosure to the first receiving system and a second subset of group identity information is selected from the group identity information for disclosure to a second receiving system, the first subset being different from the second subset~~, and a digital signature for the group~~; and

a send module transmitting the group certificate to establish the new group identity at [[a]] the first receiving system.

10. (Currently Amended) The apparatus of claim 9 further comprising:

an attach module attaching a group membership certificate to a message originated by a sender;

the send module transmitting the message to the first receiving system to establish the sender as a member of the new group at the first receiving system.

11. (Previously Presented) The apparatus of claim 10 further comprising:

a membership ID generate module generating a membership certificate having at least a public key of the sender and a digital signature for the new group;

a save module, responsive to the membership ID generate module, storing the membership certificate;

a retrieve module retrieving the membership certificate from the save module and providing the membership certificate to the attach module.

12. (Currently Amended) The apparatus of claim 10 further comprising:

a first receiving system, comprising a processing unit and computer storage media, the computer storage media encoding modules for execution by the processing unit, including:

a receive module at the first receiving system receiving the membership certificate; and

an accept module at the first receiving system detecting whether to accept the membership certificate.

13. (Previously Presented) The apparatus of claim 12 further comprising:

an assign module assigning a security identification to communications from the sender based on the new group associated with the membership certificate if the membership certificate is accepted by the accept module.

14. (Currently Amended) The apparatus of claim 10 further comprising:

a personal ID generate module generating a personal certificate having at least a public key of the sender and a digital signature by the sender; and

the send module transmitting the personal certificate to establish the sender's identity at the first receiving system.

15. (Currently Amended) The apparatus of claim 12 further comprising:

a personal ID generate module generating a personal certificate having at least a public key of the sender and a digital signature by the sender;

a receive module at the first receiving system receiving the certificates;

an accept module at the first receiving system detecting if the certificates are to be accepted;

an assign module assigning a security protocol to communications from the sender based on a group identity associated with the membership certificate if the membership certificate is accepted by the accept module;

the send module transmitting the personal certificate to establish the sender's identity at the first receiving system; and

the assign module assigning a security protocol to communications from the sender based on personal identity associated with the personal certificate if the personal certificate is accepted by the accept module.

16. (Currently Amended) A computer storage medium readable by a computing system and encoding a computer program of instructions for executing a computer process for establishing a new group identity in communications between an initiating system and a first receiving system, said computer process comprising:

generating at the initiating system a group certificate comprising at least a group use policy that expresses a privacy policy providing instructions as to how a first subset of group identity information may be used at the first receiving system, wherein the embedded use policy is stored with the first subset of group identity information, a group public key and a digital signature for the group signed with a group private key associated with the group public key, and wherein the first subset of group identity information is selected from group identity information for disclosure to the first receiving system and a second subset of group identity information is selected from the group identity information for disclosure to a second receiving system, the first subset being different from the second subset;

sending the group certificate to the first receiving system to establish the new group identity at the first receiving system;

sending a membership certificate to the first receiving system to establish [[the]] an originator as a member of the new group at the first receiving system;

generating a personal certificate having at least a public key of the originator, a personal use policy that expresses a personal privacy policy providing instructions as to how personal identity information may be used, wherein the embedded personal use policy is stored with the personal identity information, and a digital signature for the originator signed by the originator with a private key associated with the public key of the originator; and

sending the personal certificate to establish the personal identity of the originator at the first receiving system.

17. (Cancelled)

18. (Previously Presented) The computer readable medium of claim 16 wherein the process further comprises:

creating the membership certificate at the initiating system, the membership certificate having at least a public key of the originator and a digital signature signed using the group private key.

19. (Currently Amended) The computer readable medium of claim 16 wherein the process further comprises:

receiving the membership certificate at the first receiving system; and

testing acceptance of the group identity received in the membership certificate.

20. (Previously Presented) The computer readable medium of claim 19 wherein the process further comprises:

assigning a security protocol to communications from the originator based on the new group identity if the membership certificate is accepted by the act of testing.

21. (Cancelled)

22. (Currently Amended) The computer readable medium of claim 16 wherein the process further comprises:

accepting the identity information in the certificates received at the first receiving system if the certificates have been previously accepted;

assigning a security identification to communications from the originator based on the first subset of group identity information if the membership certificate is accepted; and

assigning a security identification to communications from the originator based on the personal identity information of the originator if the personal certificate is accepted.